ISSN 2658-5014 (Print) SIIT ISSN 2686-7044 (Online)
2025. Vol. 7, no. 3 (22), pp. 74–86 http://siit.ugatu.su
SYSTEMS ENGINEERING AND INFORMATION TECHNOLOGIES
Scientific paper

UDC 621.9.047 DOI 10.54708/2658-5014-SIIT-2025-no3-p74 EDN WOMBOT

Blockchain-Powered Agri-Security for Corn Supply Management

KAJAL JAIN • SANJEEV RANA

Abstract. Due to the ever-growing safety and contamination concern regarding products like wheat, rice, and maize in their respective government supply chains, traceability in their chain is highly demanded. The original traceability process for such products from government financial aid to raw material to final consumer is insecure, complex and costly. The existing food supply chain methodology lacks scalability and efficiency in the case of agricultural products. Apart from this, the consumers also don't have the resources or tools used in assessing the quality of such products for detecting flaws or contamination and making a decision whether the product is safe for consumption or not. Blockchain technology provides a revolutionary solution in upgrading traceability and security for the governmental as well as non-governmental agricultural supply chain. This paper proposes a framework that uses smart contracts to track and monitor all interactions and transactions within the government corn agricultural ecosystem. This model ensures the implementation of information relating to the product's real-time availability due to better decision-making in the supply chain. Each transaction will be recorded and stored in the public ledger of the blockchain, ensuring full transparency in its operations. The Blockchain-enabled Secure and Immutable Grain Chain model (BSIGC) framework for e-government supply chain will allow for the immutable, efficient and secure monitoring of corn agricultural goods for safety and quality. A performance analysis shows that this framework performs well on cost efficiency, security, scalability and low computational overhead as compared with conventional ones.

Keywords: blockchain, Ethereum, E-government services, food security and traceability, smart contract, consensus algorithm, supply chain.

INTRODUCTION

Public safety in agriculture can be safeguarded by overseeing agricultural production and ensuring the effectiveness and security of supply chain logistics [Bos13]. Concerns about food quality and the potential for contamination have sparked renewed interest in improving the security and traceability of agricultural supply chains [Coo97]. Additionally, authentic tracking and national certifications are essential for agricultural products traded internationally. Ensuring traceability requires the specific identification of sources and the exchange of data across the supply chain for collecting, sharing, and managing critical information. Managing the complexity of the data produced, packaged, and handled by multiple intermediaries is a significant challenge in the agricultural and food supply chain [Sal19]. Incidents of food contamination and the subsequent impact on public health underscore the importance of traceability as a key policy tool for monitoring and safeguarding food safety. To improve the traceability of food supply chains in agriculture, it has been suggested that advanced data collection methods like barcodes and RFID technology should be implemented [Bha21]. However, current traceability systems in agricultural supply chains often operate with centralized data management, which makes them vulnerable to data manipulation and management errors [Lat22]. In cases where contamination occurs, rapid removal of the affected products from the supply chain requires tight coordination between various stakeholders [Men17]. While certain stages of the supply chain may be traceable, sharing data across all phases is often a slow and complex process. As a result, many researchers have explored alternative approaches to ensure that the traceability of resources is both efficient and secure [Cas19]. One such approach involves blockchain technology, a decentralized ledger that prevents unauthorized alterations. Blockchain consists of blocks that record transactions, and each block contains unique hash, stored data, and the hash of the previous block (except for the initial block, called the genesis block) [Tha17].

Recommended for publication by the Program Committee of the X International Scientific Conference ITIDS'2024 "Information Technologies for Intelligent Decision Support", Ufa–Baku–Chandigarh, November 12–14, 2024.

The hash acts as a digital signature for each block, and any changes to the block would alter its hash, ensuring the integrity of the data. The linkage between blocks through hashes makes the system highly secure. In this context, Ethereum blockchain will be the focus, as it can function in both public and private capacities, unlike other types of blockchain, which are primarily public [Wes19]. The execution of smart contracts on Ethereum is governed by "gas," a token used to compensate miners for validating transactions. Every transaction and smart contract require sufficient gas to be processed; otherwise, they may fail to execute. To maintain the security of a blockchain, blocks must reach a consensus [Toy20], preventing unauthorized modifications. Among the various consensus algorithms, this work will focus on Proof of Authority [Fah23]. Blockchain's increasing relevance is largely due to its ability to establish trust among stakeholders through transparent and immutable transactions in the supply chain. As a trustworthy, secure, traceable, and tamper-resistant technology, blockchain has significant potential for managing government agricultural and food supply chains, which involve a complex network of entities, including farmers, industries, processors, consumers and other stakeholders [Che21].

LITERATURE REVIEW

This study aims at developing a technological framework that shall be effective across government sector and accessible along the food supply chain to facilitate continuity and consistency. Other studies also present frameworks of agricultural supply chains that point out the use of ICT to support farmers' decision capabilities by providing critical information. The relative amount of information available to the users, especially farmers involved in other types of farming activities, is larger than for non-users. Systems leverage the increased usage of personal computers and reduced costs of digital communication tools. Other technologies include RFID and blockchain, whose integration with others increases traceability and adds trustability to the agri-food supply chain. It collects and shares actual-time information about agricultural products so that food safety is ensured through safe storage, exchange, and monitoring of data [Ge15]. However, such frameworks still remain vulnerable to matters such as system fragmentation and the centralized administration aspect that could potentially manipulate data. Blockchain, being a decentralized network, is quite apt with distributed economic networks and gives a clear infrastructure for supply chains. It has been termed as a revolutionary tool to upgrade traceability within farm products. Various versions of public and private blockchain frameworks have been proposed to facilitate the agricultural supply chain by establishing transparency and security [Luu16]. While blockchain is highly supportive, implementation with double-chain architecture may turn out to be cost-effective but experimentally inefficient. Recent studies have also targeted food industry supply chain and credit evaluation systems [Ali11]. These systems help consumers to get the necessary information and are pretty good tools for government agencies and food safety authorities. In this regard, a number of studies have developed methods for normalizing supply chains based on big data and blockchain technology. For instance, authors in [Fot17] proposed strategies to normalize supply chain activities using big data and blockchain technology. The blockchain is considered among the brightest techs because it can potentially be the next major technological revolution [Jai24]. Going forward, many companies are now looking at applying blockchain to improve the traditional food systems by creating a distributed, immutable record. For instance, IBM formed a partnership in 2017 with international large food companies like Nestle and Walmart to implement blockchain within the food supply chain [Yak22]. In China, JD.com and Tsinghua University collaborated in using blockchain technology in tracing food products [Mao18]. It is related to improving food safety and maximizing business deals by using secure global networks based on blockchain technology. Of course, these solutions are successful for tracing and transparency but have not yet covered monitoring and managing funds supplied by government and its utilization in the food supply chain. At the present time, more attention is paid to traceability throughout the global food production chain. For corn products, the research indicated that traceability and tracking in the supply chain are highly crucial and that consumer opinion on usability should be included as well. A new approach has been proposed through

the adoption of Ethereum blockchain and smart contracts to successfully carry out business activities in the corn supply chain. This does not depend on centralized authorities or even third-party intermediaries for transaction databases, which thus enhances the quality and security of the data stored. Table 1 shows the related work done in agricultural fields like rice, wheat, soyabean etc.

Table 1

Related work in the field of agricultural field

Reference	Objective	Technique Used	Limitations
[Che21, Niz18]	To achieve transparency and traceability.	Double-chain blockchain concept is used.	Cost-effective, inefficient, double spending.
[Ali11, Per19]	To achieve transparency and traceability.	Blockchain Technology is used.	Cost-effective and inefficient.
[Tha17, Atz17]	To achieve transparency and traceability.	ICT gadgets are used.	Central point of failure, involvement of central controller, and cost-effective.
[Fah23, Lin20]	To achieve traceability and reliable information.	Technique of RFID and blockchain.	It is susceptible to system fragmentation and central administration.
[Sal19, Zhe20, Opa03]	To analyze farmers' decision-making in supply chain.	ICT gadgets are used.	Central point of failure, involvement of central controller, cost-effective and scalability issues.
[Bha21, Wes19]	To achieve transparency and traceability.	Blockchain.	Cost-effective and inefficient.

PROBLEM STATEMENT

The origin of a commodity from government to raw materials to its end consumer can hardly be tracked, and it is also very expensive. Traditional methods of managing the food supply chain have proven inadequate in providing a scalable, cost-effective solution. A more robust system is needed, which monitors information regarding the source, farming practices, and safety of products throughout the e-government supply chain without being dependent on third parties or centralized authorities. In the case of agricultural products' processing and procurement, there should be a well-structured effective and workable system for assessing the quality and safety of the product. This would, therefore, equip stakeholders such as consumers with knowledge of conducting safe business in the agri-food supply industry and efficiency in providing economic incentives.

Problem Statement

This work provides the means to showcase how Ethereum blockchain technology and smart contracts can be effectively applied to monitor government agriculture supply chain. It proposes a model of accountability within corn supply chains using a basis on Ethereum blockchain.

Figure 1 outlines commodity flow in the corn supply chain, indicating key stakeholders and their roles.

The main contributions of this paper are:

1. Design a framework of the application of Ethereum Smart Contracts to improve traceability and transparency in the government-based corn supply chain.

2. Expanding on this framework to explain significant characteristics of our blockchain approach, which focuses on communication between varied stakeholders who are involved in the supply chain.

3. The proposed smart contract algorithms are discussed and analyzed in order to ensure that the right interactions and utilization of funds supplied by government occurred among the relevant parties within the corn supply chain.

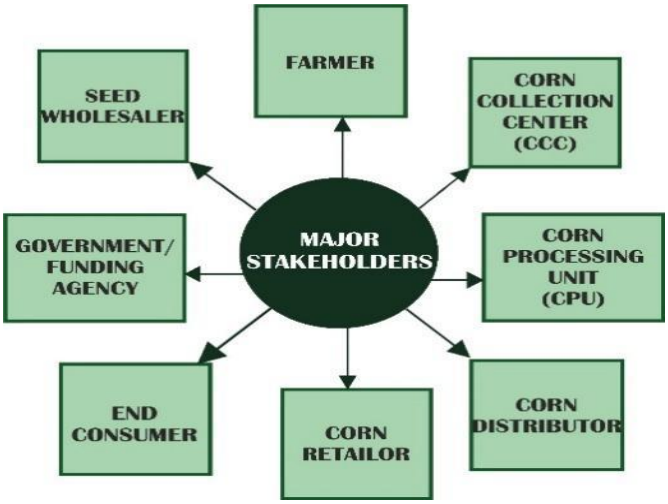

Fig. 1. Major stakeholders involved in corn supply chain management.

RESEARCH METHODOLOGY

System Model

The proposed architecture Blockchain-enabled Secure and Immutable Grain Chain model (BSIGC) model operates on a proprietary Ethereum blockchain network. Nodes are available across the private/public network; they authenticate transactions and then append them to the blockchain ledger, using the POA consensus mechanism in executing smart contracts. Earlier all the supply chain management systems were based on proof of Authority consensus algorithm. Any organization that can collect, validate, and process transactions may be a mining node, and these nodes maintain the data and results of transactions in a common ledger accessible to all mining nodes. Smarter contracts facilitate transactions through function calls and events, thus allowing stakeholders to observe, trace, and receive relevant updates as necessary. For instance, information about corn products is written on the blockchain. This information is linked with the expiry time of the product after which it is eradicated to make way for new transactional data. This framework promotes transparency and traceability in the corn supply chain, thus ensuring the safety of the product to consumers and rectifying any interruptions that may occur in the supply chain. Furthermore, it enables customers to give reviews of products obtained through this platform. The public ledger captures the information in a selective manner for the roles of stakeholders and hence rejects redundancy [Mao18]. Figure 2 shows the working of BSIGC model.

The process involves eight core involved stakeholders linked by smart contracts: (1) Government who supplies funds to the farmers. (2) Seed Wholesaler, a company which sells seeds of different corn varieties complying with international standards. All seed products carry standard identifiers-serialized GTIN Global Trade Identification Numbers. (3) Farmer; they will purchase the seeds from SW and plant crops while utilizing the funds provided by government/funding agencies and smart contracts using traceable identification of the seeds. (4) Agricultural producers have the responsibility of constantly updating and recording information on crop status in a distributed tamper-proof log or ledger as is presented by the Inter Planetary File System (IPFS) [Li23]. The hash of this log is recorded on the blockchain for later extraction [Agg19] of corn crop output while assessing the number, quality, weight and type. Environmental factors like temperature, humidity and time of storage are monitored during the storage time. (5) Corn Processing Unit take corn from corn collector center and sells processed products to the distributors. (6) Corn Distributor acquire agricultural products from the CPU in order to further disseminate them among the retailers or bring them directly to the customers. (7) Corn Retailer. The CD sells the final products with STI to the CR who sell them in smaller quantities to the end-users. (8) The end consumer purchases finished corn

products from the CR for direct use, and all the products have been attached with both STI and GTIN for traceability purposes.

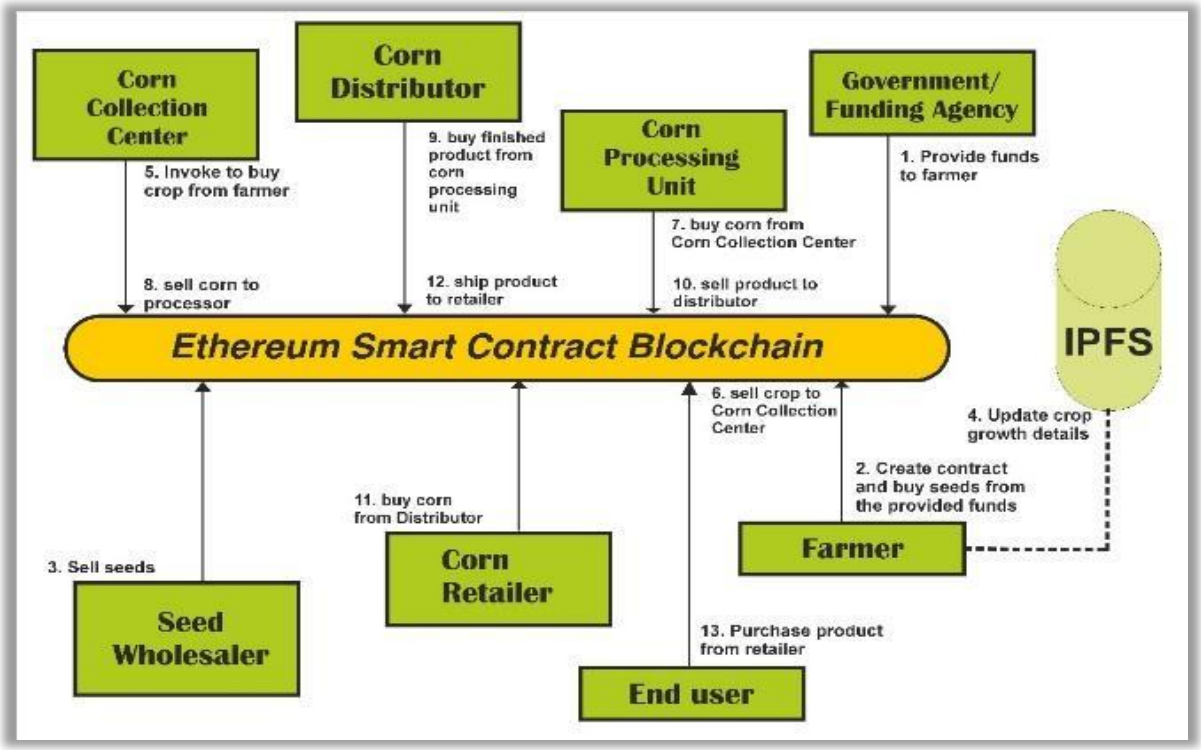

Fig. 2. BSIGC model for corn supply chain management.

Every participant must be registered within the framework, authenticate itself, and then prove its identity by participating in the food chain process and also own a unique Ethereum account with its own Ethereum address (EA), through which it identifies the stakeholder within the network. Such EAs include public and private keys used in signing and verification of data in a transaction. Traceable functionality ensures that the parties involved have access to information that is, at the same time, immutable and verifiable, thus there is no need for a central authority [Sin24]. This characteristic spread throughout all the supply chains would allow tracking of total volume of corn produced and traded among entities with verified transactions. For instance, the amount of corn traded under established conditions remains unchanged. Moreover, corn varieties meeting distinct quality specifications must not be combined for sale, as the total volume corresponding to each standard is meticulously documented. Furthermore, farmers have the capability to upload electronic records, including images of crops and details regarding land conditions, utilizing systems such as IPFS, thereby establishing a digital repository for validation purposes [Ali11]. Shipping integrity can also be quantified by using containers with sensors, like cameras, GPS, and 4G. These sensors continuously transmit updates on the condition of corn shipments, and all stakeholders have permanent access to this information through the blockchain. Identifiers can also standardize the findings regarding the physical location of a product, while participants' locations can be geotagged by using GPS sensors on shipping or storage containers.

BSIGC Framework for Agri-Security for Corn Supply Management Using Blockchain

This section delineates the operational principles underlying the BSIGC framework for government supply chain management of corn crops. First, a smart contract is developed and deployed, subsequently leading to the registration of each participating entity's EAs with the contract. When a farmer requests for funds with the government/funding agencies, farmer status “FundRequested” status updated, and after transferring funds by the government, GA status updated

as “FundTransfered”, and then farmer negotiates a possible seed supply from an appropriate SW, a farmer's status is updated to “SupplyRequested,” as shown in Algorithm 1. The contract verifies the authenticity of the farmer and ensures if he has made the payment. If the farmer is a validated participant, and payment is confirmed, his contract status is updated; meanwhile, the farmer's status is updated to “ServiceWait” along with that of the SW being updated as “SalesApproved.” At this point, the smart contract sends notifications regarding the progress to all stakeholders. In case any prerequisites are not fulfilled, the system reinstates all statuses to their initial state, and thus the transactions are cancelled.

Algorithm 1: Funds Receiving by Farmer and Buying Seeds from Seed Wholesaler (SW)

Rf is a set of all registered farmers
Ethereum Authorization(EA) of the government authority transferring the funds to the farmer is known
Ethereum Authorization(EA) of farmer is known
Ethereum Authorization(EA) of Seed Wholesaler is known
CQuantity, CSType, CSBrand, CSPrice

ContractState Created
Farmer Status: FundsRequested through Government Program
GA Status : FundsTransferred
Farmer’s Status: SupplyRequested
SW Status: Read
Consider only farmer is from Rf i.e. registered farmers
If farmer ¼ registered and SPrice ¼ paid Then
Contract status ! RequestOnProcess
Farmer status ! ServiceWait
SW status ! SalesApproved
Broadcast a notification message for the seeds sales
End
Else
Return to initial contract state and show an error
End

Algorithm 2: Selling of Corn Seeds from CCC to CPU

PCPU is the set of all registered CPU
EA of CPU is known
EA of CCC is known
CQuantity, CDatePurchased, CPPrice

ContractState: CornFromCPU
CCC Status: CornRequested
CPU Status: YieldFromFarmer
Consider only CPU is registered PCPU i.e. registered CPUs
If Cornsale ¼ Accepted and CPPrice ¼ paid Then
Contract status ! RequestApproved
CPU status ! WaitForCorn
CCC status ! CornReleaseSuccessful
Broadcast a notification message for the Corn sales
End
Else
Contract status ! RequestDenied
CPU status ! RequestNotSuccessful
CCC status ! CornReleaseFailed
Broadcast a notification message for the Corn sales failure
end
else
Return to initial contract state and show an error
End

The third stage of the framework is described in Algorithm 3.At this stage, the smart contract guarantees that only registered CRs can buy goods. In the same way, it verifies if the sale negotiations are approved, and the payment made. If these conditions are valid or fulfilled, the smart contract will be executed where the CD transfers the product to the CR. As a result, the smart contract status changes to *ProductBuyingSuccessful*, while the CD and CR status changes to *ProductSoldToCR* and *ProductDeliverySuccessful* respectively. A notification message shall be sent to all active participants concerning the selling of products to CR. However, if the conditions are not fulfilled, the smart contract status changes to *ProductBuyinDenied*, while the CD and CR status changes to *ProductRequestFailed* and *ProductDeliveryFailed* respectively. A warning message for failure is then sent to all participants.

Algorithm 3: Selling product to Corn Retailer (CR)

Input: RCR is the set of all registered CR
EA of CD is known
EA of CR is known
CQuantitySold,CDatePurchased,CDateProduced, CProductPayment
1 ContractState: CDSales
2 CD Status: CPProductReceived
3 CR Status: PreparedToBuy
4 Consider only CR is in RCR i.e. registered CRs
5 If Productsale ¼ Accepted and ProductPayment ¼ paid Then
6 Contract status ! ProductBuyingSuccessful
7 CD status ! ProductSoldToRCR
8 CR status ! ProductDeliverySuccessful
9 Broadcast a notification message for the corn product sales
10 End
11 Else
12 Contract status ! ProductBuyinDenied
13 CD status ! ProductRequestFailed
14 CR status ! ProductDeliveryFailed
15 Broadcast a notification message for the Corn product sales failure
16 end
17 else
18 Return to initial contract state and show an error
19 End

At this stage, the final consumer, who is the last participant in this system, eventually purchases the final product from the CR, Algorithm 4 defines the stage processes.

Algorithm 4: Selling Corn products to consumers

Input: RCR is the set of all registered CR
EA of CR is known
EA of Consumer is known
CQuantitySold, CDatePurchased, CSalesID and CProductID, CProductPayment
1 ContractState: SaleRequestApproved
2 CR Status: ProductDeliverySuccessful
3 Consumer Status: ReadyToPurchase
4 Consider only CR is registered RCR i.e. registered CRs
5 If CR to RCR and ProductPayment ¼ paid
Then
6 Contract status ! SoldToConsumer
7 CR status ! SalesSuccessful
8 Consumer status ! PurchaseSuccessful
9 Broadcast a notification message for the corn product sales
10 end
11 else
12 Contract status ! SaleRequestDenied

```
13  CR status ! SalesFailure
14  Consumer status ! PurchaseFailed
15  Broadcast a notification message for the product sales failure
16  end
17  else
18  Return to initial contract state and show an error
19  end
```

Date of Purchase, Sales Identification Number, and Product Identification Number are the critical variables at this stage. In this stage, the consumer's state is tagged as "ReadytoBuy," simultaneously with the smart contract state assigned as "Sale Request Accepted," and the CR state is captured as "Product Delivery Successful." The conditions that should be met at this stage include the constraint that only products listed by the CR are available for consumers to use, as well as the fact that the intended payment has indeed been made. If these conditions are satisfied, the smart contract will update its status to "SoldtoConsumer," and statuses of CR as well as of Consumer would be updated to "Sales Successful" and "Purchase Successful," respectively. The parties involved should be sent notification that the product is sold to the consumer. If any of the above conditions are not met, then the status of a smart contract shall turn into "Sale Request Denied," and statuses of CR and Consumer would be updated into "Sales Failure" and "Purchase Failed." Afterwards, each participant should receive a warning message that the process failed.

Implementation, Results, and Analysis

This section begins with the experimental setup and deployment followed by results and analysis subsections to measure the logic and performance of the BSIGC framework.

Experimental setup and deployment

An experiment to test the proposed model for effectiveness by divide-and-conquer approach was carried out. The implementation on Remix IDE used Solidity language while interacting with Ethereum using MetaMask, an Ethereum wallet, as well as Chrome extension, which simplified some interactions with Ethereum networks. Remix IDE also equips the user to test and debug the smart contracts before they are actually deployed. Sepolia testnet was used to simulate blockchain scenarios when testing. The testnet has run on Proof of Authority to allow a more realistic simulation of the blockchain. All Ethereum nodes in the testnet were accessed by the gateway service called Infura [Mao18]. To cut down on testing and swap between different testnets, the Truffle Framework was used. In the validation process, tests had been conducted on functions and modifiers for smart contracts that only authenticated Ethereum addresses would perform certain actions [Oli20]. The logs were checked to ensure that information was flowing properly, and data was accurate.

Results and Analysis

This section will evaluate the feasibility of the BSIGC framework in terms of the security requirements and cost considerations to establish whether the framework is feasible for deployment in the real world. First, it discusses the security characteristics in detail that could potentially be compromised in smart contracts and then moves to explore the challenges in future research. After that, the BSIGC framework will be compared against the existing solution, and the generalization along with the importance of the research will be discussed.

Security Analysis

Privacy. Privacy guarantees that communications between two parties are strictly private and not disclosed to third parties. Whereas it is important that the privacy of communications should be maintained permitting the access to digital information only to the authorized parties, our solution encompasses message encryption and decryption through an SSL session, which would be established after a trusted handshake that would verify the parties participating. Centralized Public Key Infrastructure architecture makes this lacking in adequate transparency and overly dependent on Certificate Authorities to facilitate cryptographic key distribution. In contrast, using the Ethereum

blockchain allows for eschewing a PKI structure for encryption. With this regard, each party is assigned an Ethereum Address containing asymmetric public key pairs used to encrypt messages being passed along the SSL session.

Credibility. All communication between the users on the Ethereum network is encrypted and tamper-proof. In addition to this, time stamps along with specific attributes for EAs are maintained on the blockchain to ensure the integrity of the interaction of different entities. Consequently, this mechanism offers protection against both MITM attacks and replay attacks.

Authorization. Only privileged stakeholders have access to the entire set of functionalities offered by the smart contract. In case an authentic call initiator is identified as fraudulent, an error will be produced, leading to a rollback of all states. Moreover, further interactions between stakeholders rely on an authentication handshake that ensures a secure SSL connection.

Non-repudiation. All transactions and events are recorded systematically in the public ledger of Ethereum, ensuring that the calls are accurately logged and cannot be altered by the originator. For this reason, no one can deny their actions since all the data is stored within an immutable public ledger. Additionally, when a malicious user attempts to replicate a stakeholder's EA, they will be detected since they lack the private key, which is required to sign the message.

Cost Analysis

Every transaction that is carried out on the Ethereum blockchain incurs transaction costs. Besides the transaction and execution costs, the Remix IDE logs include other information. For each transaction, gas is measured in Gwei and paid in Ether. Higher values of Gwei attached to a transaction mean that miners will prioritize it. The ETH Gas Station provides diverse transaction speeds based on gas prices. Gas costs should be considered during the development of a smart contract, to avoid being charged extra for doing nothing. There are several factors which influence the cost of transactions, like loops, arrays, mappings, variable storage, and data types. The key is a very practical and efficient solution. The approach is that we use leverages immutability by using events and logs of the blockchain instead. We are also aware of the current high gas prices, i.e. 10–9 ETH, due to network congestion since gas rates fluctuate depending on time and day. The actual transaction cost depends on the gas price of the Ethereum client.

Smart Contract Vulnerability Analysis

The analysis of the Smart Contracts that are incorporated in the BSIGC framework was carried out using the Slither Security Analysis Tool with its results shown in Table 2.

Table 2

Vulnerability Analysis Report

Features	Existing Model [Sal19]	BSIGC Model
Satisfaction feedback	No	Yes
Cost Analysis	No	Yes
Implementation and Testing	No	Yes
Security analysis	No	Yes
Vulnerability analysis	No	Yes
Low computational cost	No	Yes

The tool analyzes EVM bytecode and comes back with very detailed smart contract interaction mapping. Its analysis results showed that Smart Contracts are secure with no vulnerabilities [Per19]. There are no unchecked exceptions that may lead to integer transaction underflow or integer overflow. All tests were performed for supplying gas during the execution phase such that the possibility of reentrancy attacks was much reduced. From the results, it was concluded that there was no concern about the framework in terms of timestamps or interdependent transactions.

A Comparison of the BSIGC Framework with Existing Agricultural Food Supply Chain Solutions

Comparison of the framework of this paper with the existing discussion by authors is presented in Table 3. In terms of achieving data integrity, information access, transparency, and traceability regarding corn supply, current techniques rely on smart contracts and consensus mechanisms to address these issues in corn supply traceability problems. The authors discuss the feasibility of their approaches as well toward the solution of real-world problems, showing minimal technical requirements. For example, author [Sal19] discuss possibilities to use smart contracts on the Ethereum platform in conjunction with IPFS for storing data; they use several smart contracts to represent each role in a supply chain [Sin23]. This increases computational overhead with respect to their proposed solution.

Table 3

Comparison of the BSIGC Framework with Existing Works

Parameters	Vulnerability in Existing Model [Sal19]	Vulnerability in BSIGC Model
EVM Code Coverage	62%	32%
Integer Underflow	Moderate	Low
Integer Overflow	Low	Moderate
Call Stack Depth Attack Vulnerability	Moderate	Low
Transaction Ordering Dependence	Moderate	Low
Time Stamp Dependency	Low	Moderate

Due to the public aspect of Ethereum platform, it is widely used in different applications; therefore, any stakeholder can easily join the network. Main strengths of Ethereum are an extremely vast number of developers, a very well-established ecosystem of dApps, and the native cryptocurrency ETH. Scalability and high transaction costs (the term used to describe them is gas fees) remain the most significant weaknesses for Ethereum. Figure 3 shows the comparison between various blockchain platforms.

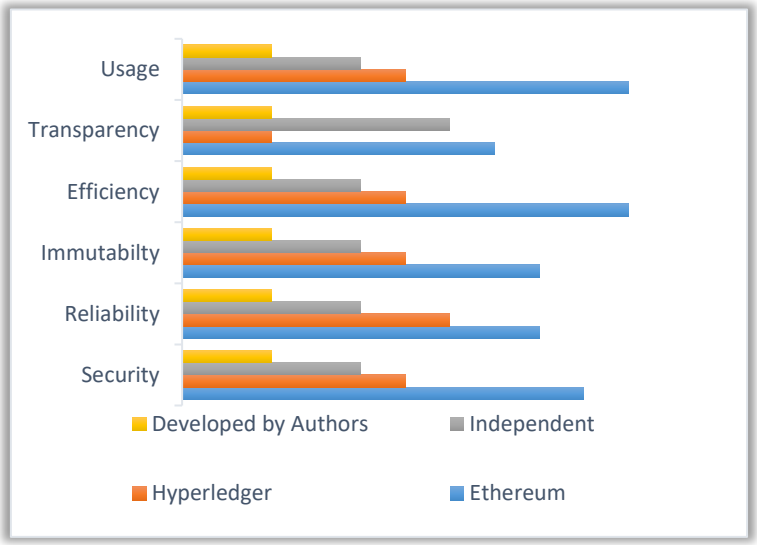

Fig. 3. Comparison of the Ethereum platform with other blockchain platforms.

DISCUSSION AND CONCLUSION

To this end, we developed and tested our BSIGC framework on Ethereum blockchain platform in response to high demand in the supply chain and agriculture sectors. Adding data encryption with the transactions in a blockchain system, companies are compelled to conduct their transactions in house. This solution can be tailored to suit the varied needs of various firms. The smart contracts that have been designed here are very flexible and hence can easily be deployed on any kind of blockchain; therefore, it ensures immediate execution with respect to the transactions along with privacy, transparency, and safety. The model efficiently traces and tracks the food supply chain concerning corn production monitors, ensures delivery process by getting all parties to adhere to the set supply chain regulations. All parties involved in any given malpractice are identified in the supply chain, thereby minimizing the risk of food contamination. All these are corn crops, which have common agronomic characteristics; hence, this study is relevant to any other corn supply chains because the model showed its efficiency in tracing corn production. For example, government agencies may apply such findings tracing supply chains of wheat beans, millet, and so forth. Therefore this research can be used as a template to monitor and track any corn commodity's supply chain. Other beneficiaries of this program are Corn processors, farmers, agronomists, agricultural agencies, merchants, food regulators, and crop scientists. We wrote our smart contracts in the language called Solidity for better compatability with the Ethereum blockchain; our general methodology applied easily to other blockchain systems with minimal effort.

REFERENCES

[Agg19] Aggarwal S., Chaudhary R., Aujla G. S., Kumar N., Choo K. K. R., Zomaya A. Y. Blockchain for smart communities: applications, challenges and opportunities // Journal of Network and Computer Applications. 2019. Vol. 144(5). P. 13–48. DOI: 10.1016/j.jnca.2019.06.018. EDN: MQTESQ.

[Ali11] Ali J., Kumar S. Information and communication technologies (ICTs) and farmers' decision-making across the agricultural supply chain // International Journal of Information Management 2011. Vol. 31(2). P. 149–159. DOI: 10.1016/j.ijinfomgt.2010.07.008.

[Atz17] Atzei N., Bartoletti M., Cimoli T. A survey of attacks on Ethereum smart contracts (SoK). In: Proceedings of the 6th International Conference on Principles of Security and Trust. Vol. 10204. Berlin: Springer, 2017. P. 164–186. DOI: 10.1007/978-3-662-54455-6_8.

[Bha21] Bhat Sh. A., Huang N.-F., Sofi I. B., Sultan M. Agriculture-food supply chain management based on blockchain and IoT: A narrative on enterprise blockchain interoperability // Agriculture. 2021. Vol. 12. No. 1. P. 40. DOI: 10.3390/agriculture12010040.

[Bos13] Bosona T, Gebresenbet G. Food traceability as an inteCRal part of logistics management in food and agricultural supply chain // Food Control. 2013. Vol. 33(1). P. 32–48. DOI: 10.1016/j.foodcont.2013.02.004.

[Cas19] Casino F., Kanakaris V., Dasaklis T. K., Moschuris S., Rachaniotis N. P. Modeling food supply chain traceability based on blockchain technology // IFAC-PapersOnLine. 2019. Vol. 52(13). P. 2728–2733. DOI: 10.1016/j.ifacol.2019.11.620.

[Che21] Chen L., Cong L. W., Xiao Y. A brief introduction to blockchain economics / Ed. by K. R. Balachandran. Information for efficient decision making: Big data, blockchain and relevance. World Scientific Publishing, 2020. P. 1–40. DOI: 10.2139/ssrn.3442691.

[Coo97] Cooper M. C., Lambert D. M., Pagh J. D. Supply chain management: more than a new name for logistics // The International Journal of Logistics Management. 1997. Vol. 8. No. 1. P. 1–14. DOI: 10.1108/09574099710805556.

[Fah23] Fahim Sh. S., Rahman K., Mahmood Sh. Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV // International Journal of Mathematical Sciences and Computing. 2023. Vol. 3. P. 46–57. DOI: 10.5815/ijmsc.2023.03.04. EDN: TFFTVU.

[Fot17] Foth M. The promise of blockchain technology for interaction design. In: ACM International Conference Proceeding Series. New York: Association for Computing Machinery, 2017. DOI: 10.1145/3152771.3156168.

[Ge15] Ge H., Gray R. S., Nolan J. F. Agricultural supply chain optimization and complexity: A comparison of analytic vs simulated solutions and policies // International Journal of Production Economics. 2015. Vol. 159(2). P. 208–220. DOI: 10.1016/j.ijpe.2014.09.023.

[Jai24] Jain K., Rana S. A review on blockchain-based paradigm for the management of digital assets in healthcare. In: 2024 IEEE 5th India Council International Subsections Conference (INDISCON). IEEE, 2024. P. 1–6. DOI: 10.1109/INDISCON62179.2024.10744254.

[Lat22] Latino M. E., Menegoli M., Lazoi M., Corallo A. Voluntary traceability in food supply chain: a framework leading its implementation in Agriculture 4.0 // Technological Forecasting and Social Change. 2022. Vol. 178. Art. 121564. DOI: 10.1016/j.techfore.2022.121564. EDN: XOAUNP.

[Li23] Li L., Jin D., Zhang T., Li N. A secure, reliable and low-cost distributed storage scheme based on blockchain and IPFS for firefighting IoT data // IEEE Access. 2023. Vol. 11. P. 97318–97330. DOI: 10.1109/ACCESS.2023.3311712.

[Lin20] Lin W., Huang X., Fang H., Wang V., Hua Y., Wang J., Yin H., Yi D., Yau L. Blockchain technology in current agricultural systems: from techniques to applications // IEEE Access. 2020. Vol. 8. P. 143920–143937. DOI: 10.1109/ACCESS.2020.3014522. EDN: BSNGNE.

[Luu16] Luu L., Chu D. H., Olickel H., Saxena P., Hobor A. Making smart contracts smarter. In: Proceedings of the ACM Conference on Computer and Communications Security. New York: ACM, 2016. P. 254–269. DOI: 10.1145/2976749.2978309.

[Mao18] Mao D., Wang F., Hao Z., Li H. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain // International Journal of Environmental Research and Public Health. 2018. Vol. 15(8). Art. 1627. DOI: 10.3390/ijerph15081627.

[Men17] Mendi A. F. Blockchain for food tracking // Electronics. 2022. Vol. 11. No. 16. Art. 2491. DOI: 10.3390/electronics11162491.

[Niz18] Nizamuddin N., Hasan H. R., Salah K. IPFS-blockchain-based authenticity of online publications / Ed. by S. Chen, H. Wang, L. J. Zhang. Lecture Notes in Computer Science. Vol. 10974. Cham: Springer, 2018. DOI: 10.1007/978-3-319-94478-4_14.

[Oli20] Oliva G. A., Hassan A. E., Jiang Zh. M. An exploratory study of smart contracts in the Ethereum blockchain platform // Empirical Software Engineering. 2020. Vol. 25. P. 1864–1904. DOI: 10.1007/s10664-019-09796-5. EDN: UVAHFG.

[Opa03] Opara L. U. Traceability in agriculture and food supply chain: A review of basic concepts, technological implications, and future prospects // Journal of Food, Agriculture & Environment. 2003. Vol. 1. P. 101–106. DOI: 10.1234/4.2003.323.

[Per19] Perez D., Livshits B. Smart contract vulnerabilities: Does anyone care [arXiv preprint] // arXiv. 2019. Art. 1902.06710. P. 1–15. DOI: 10.48550/arXiv.1902.06710.

[Sal19] Khaled S., Nizamuddin N., Jayaraman R., Omar M. Blockchain-based soybean traceability in agricultural supply chain // IEEE Access. 2019. Vol. 7. P. 73295–73305. DOI: 10.1109/ACCESS.2019.2918000.

[Sin23] Singla D., Rana S. blockchain-based platform for smart tracking and tracing the pharmaceutical drug supply chain. In: Examining Multimedia Forensics and Content Integrity. IGI Global, 2023. P. 144–172. DOI: 10.4018/978-1-6684-6864-7.ch006.

[Sin24] Singla D., Kumar S., Gulzar Y., Mir M. Sh., Gupta D., Jaziri W., Sassi N., Arora Sh. Designing and implementing a resilient immutability mechanism for enhanced supply chain management in E-healthcare systems // Frontiers in Sustainable Cities. 2024. Vol. 6. Art. 1403809. DOI: 10.3389/frsc.2024.1403809.

[Tha17] Thanapal P., Prabhu J., Mridula J. A survey on barcode RFID and NFC // IOP Conference Series: Materials Science and Engineering. 2017. Vol. 263. No. 4. Art. 042049. DOI: 10.1088/1757-899X/263/4/042049.

[Toy20] Toyoda K., Machi K., Ohtake Yu., Zhang A. N. Function-level bottleneck analysis of private proof-of-authority Ethereum blockchain // IEEE Access. 2020. Vol. 8. P. 141611–141621. DOI: 10.1109/ACCESS.2020.3011876. EDN: OBYXLK.

[Wes19] Westerkamp M., Victor F., Küpper A. Blockchain-based supply chain traceability: Token recipes model manufacturing processes. In: 2018 IEEE Int. Conf. iThings, GreenCom, CPSCom, and SmartData. IEEE, 2019. P. 1595–1602. DOI: 10.1109/Cybermatics_2018.2018.00267.

[Yak22] Yakubu B. M., Latif R., Yakubu A., Khan M. I., Magashi A. I. RiceChain: Secure and traceable rice supply chain framework using blockchain technology //PeerJ Computer Science. 2022. Vol. 8. Art. e801. DOI: 10.7717/peerj-cs.801. EDN: IKGPTW.

[Zhe20] Zheng Z., Xie Sh., Dai H.-N., Chen W., Chen X., Weng J., Imran M. An overview on smart contracts: Challenges, advances and platforms // Future Generation Computer Systems. 2020. Vol. 105. 475– 491. DOI: 10.1016/j.future.2019.12.019. EDN: LWJAYY.

METADATA | МЕТАДАННЫЕ

The article was received by the editors on January 27, 2025
Поступила в редакцию 27 января 2025 г.

Название: Агробезопасность на основе блокчейна для управления поставками кукурузы.

Аннотация: Из-за постоянно растущей обеспокоенности безопасностью и загрязнением таких продуктов, как пшеница, рис и кукуруза в соответствующих государственных цепочках поставок, возможность отслеживать движение подобных продуктов крайне востребована. В текущем виде процесс отслеживания подобных продуктов (от выделения государственной финансовой помощи до производства/обработки сырья и доставки товара до конечного потребителя) является небезопасным, сложным и дорогостоящим. Существующая методология цепочки поставок продовольствия не имеет масштабируемости и эффективности в случае сельскохозяйственной продукции. Помимо этого, у потребителей также нет ресурсов или инструментов, используемых для оценки качества таких продуктов для обнаружения недостатков или загрязнений и принятия решения о том, безопасен ли продукт для употребления или нет. Технология блокчейн обеспечивает революционное решение в повышении безопасности и возможности отслеживания для правительственной, а также неправительственной сельскохозяйственной цепочки поставок. В этой статье предлагается структура, которая использует смарт-контракты для отслеживания и мониторинга всех взаимодействий и транзакций в государственной сельскохозяйственной экосистеме кукурузы. Эта модель обеспечивает реализацию информации, касающейся доступности продукта, в режиме реального времени, и, следовательно, способствует более эффективному принятию решений в цепочке поставок. Согласно модели, каждая транзакция будет регистрироваться и храниться в публичном реестре блокчейна, обеспечивая полную прозрачность ее операций. Структура Blockchain Enabled Secure and Immutable Grain Chain model (BSIGC) для цепочки поставок электронного правительства позволит осуществлять эффективный и безопасный мониторинг сельскохозяйственных товаров из кукурузы на предмет безопасности и качества. Анализ производительности показывает, что эта структура хорошо работает с точки зрения экономической эффективности, безопасности, масштабируемости и низких вычислительных затрат по сравнению с обычными.

Ключевые слова: блокчейн, Ethereum, электронные государственные услуги, продовольственная безопасность, отслеживание товаров, смарт-контракт, алгоритм консенсуса, цепочка поставок.

Язык статьи: Английский.

About the authors | Об авторах

Kajal Jain
Maharishi Markandeshwar (Deemed to be University), India. Research Scholar (Ph.D) in the Department of Computer Science and Engineering. Her research interests include Blockchain Technology, Computer Network and Security.
E-mail: kajal.mittal@mmumullana.org

Sanjeev Rana
Maharishi Markandeshwar (Deemed to be University), India. Ph.D. (CSE), M.Tech. (IT), B.Tech. (Computer Eng.), is currently the Founder Director, Centre for Distance & Online Education and Professor (CSE); his areas of interests include Blockchain Technology, Cyber Security, Cloud Computing, Big Data & Analytics, Network Security & Management.
E-mail: dr.sanjeevrana@mmumullana.org

Каджал Джайн
Махариши Маркандешвар (университет), Индия. Научный сотрудник (Ph.D) на кафедре компьютерных наук и инженерии. Иссл. в обл. технологии блокчейна, компьютерных сетей и безопасности.
E-mail: kajal.mittal@mmumullana.org

Санджив Рана
Махариши Маркандешвар (университет), Индия. Ph.D (CSE), магистр (IT), бакалавр (комп. инженерия). Директор Центра дистанционного и онлайн-образования, профессор (CSE). Иссл. в обл. технологии блокчейна, кибербезопасности, облачных вычислений, больших данных и аналитики, сетевой безопасности и управления.
E-mail: dr.sanjeevrana@mmumullana.org